

APPENDIX 14

Paul C. Czarapata
Fermi National Accelerator Laboratory
PO Box 500 MS220
Batavia, IL 60510

June 2, 1995

Dr. Stephen Musolino
Brookhaven National Laboratory
Upton, New York 11973-5000

Dear Stephen:

First, on behalf of the review committee and myself, I would like to thank you and your colleagues for your gracious hospitality. I personally find it rewarding and refreshing to see new facilities and new ideas presented. I submit to you the final report of the review committee for the Personnel Safety System at RHIC. The committee has taken the additional time to offer, hopefully clarify, text at the end of the report to identify why certain items were questioned. We wish you and your staff continued success. If I may be of service again please do not hesitate to call.

Sincerely,



Attachments

final committee report

Committee Report On The RHIC Personnel Safety System at Brookhaven National Laboratory

March 7-9, 1995

Committee Members:

Paul C. Czarapata - Chairman, FNAL

Howard Casebolt, FNAL

Tom Dickinson, BNL

John Forrestal, ANL

Henry Robertson, CEBAF

TABLE OF CONTENTS

CHARGE TO THE COMMITTEE	3
EXECUTIVE SUMMARY	4
RECOMMENDATIONS AND COMMENTS	5
DISCUSSION	11
ATTACHMENTS	15

Charge to the Committee

The following charge to the committee was given by Dr. Stephen Musolino, Assistant to the Head, ES&H, RHIC on behalf of Dr. Satoshi Ozaki, Project Head, RHIC:

- Review the design basis, architecture and implementation of the RHIC Personnel Safety System.
- Assess whether the system has achieved an adequate and reliable level of redundancy.
- Assess whether the planned conceptual approach of the ^{Functional}~~fundamental~~ tests will ensure the adequacy of the system test procedures.
- Compare the proposed scheme at the system level to the Laboratory and Project design requirements and to the statutory requirements in DOE Order 5480.25 and the recommendations in the DOE Guidance to the Order.
- Provide the Project with expert guidance to improve the final design so that it can be operated to provide the maximum margin of safety to personnel.
- Present the major findings, any recommendations for improvement that are at the system level and a first draft of the report at the exit meeting.

Executive Summary

At the request of the RHIC Project Leader, a review of the RHIC Personnel Safety System was conducted by this committee. We determined it was not possible to give a complete assessment of all operational details of the system since many of the procedural issues have not been developed. In this report we offer recommendations, observations and concerns as we have found them.

Among our recommendations are:

1. Separate the ODH and Radiation Safety Systems
2. Review the interaction of ODH and Fire Protection Systems
3. Implement Configuration Control Plan for ODH System
4. Reject the concept of Fail Soft to one protection loop.
5. Implement Controlled Access Procedures
6. Implement Configuration Control Plan for Personnel Safety System
7. Accept and encourage "Reachback" of Critical Devices
8. Reject the concept of Feed Forward
9. Fully isolate systems in overlap areas
10. Provide system test modes but do not compromise safety
11. Provide diverse method of control for critical devices
12. Provide standardized alarms across the AGS and RHIC
13. Adopt programming standards for PLC's
14. Review the need for dual Uninterruptable Power Supplies
15. Adopt more traditional Gate and Crash switch sensing
16. Reject Adaptive Gate Monitoring
17. Provide thorough test procedures

Recommendations and Comments

The following recommendations and comments reflect the consensus opinion of the committee. Items which are advisory comments rather than concerns are noted as such in the text.

1. The committee recommends that the function of the Oxygen Monitoring system not be integrated into the RHIC Radiation Safety System PLC's. The committee recognizes the importance of the ODH system and feels the two systems serve critical but separate functions. It is believed that the additional complications to the software, configuration control, and testing of the Personnel Safety Systems warrant independent systems. The added cost of an independent system is probably small compared to the downtime incurred for the testing and verification of a combined system.
2. RHIC management should review the relationship of the Oxygen Monitoring System and the Fire Detection/Protection System with respect to the control of the ventilation system. The review should take into account the possible cross response of the systems given a fire or helium release. A fire ionization detector may be activated by a helium release and, similarly, an oxygen sensor may alarm in the event of a fire.
3. Since the vent fans are required to reduce the ODH classification to Class 0, the fans must have strict configuration control. The fans must be monitored for proper operation and be tested as a part of the Oxygen Monitoring System.
4. A proposal was made that would allow the RHIC complex to operate with only one Personal Safety System loop active while the second loop underwent necessary repair. The committee categorically *rejects* this proposal. It is the feeling of the committee that this would expose the system to possible failure. The exact operating status of all

other system components in the operating loop is, at best, unknown and therefore cannot be guaranteed functional.

5. It is recommended that the Controlled Access Procedures, including types of keys, their function, and control, be clearly defined soon to allow the necessary integration into the Personnel Safety System.
6. The committee recommends to the AGS/RHIC management that a strict and thorough Configuration Control Policy be implemented. This policy should address but not be limited too:
 - a. Keys - usage, responsibilities, replacement procedures.
 - b. Hardware Systems - Jumpers/temporary by-passes, PLC networking, computer interfaces.
 - c. Software - access to PLC "programming key", control of revisions, review process, approvals.
 - d. Certification Procedures/Checklists - revisions must not affect test integrity.
 - e. Documentation - functional descriptions, technical specifications, wiring, special circuits or configurations.
7. The committee feels the use of "Reachback", namely disabling upstream critical devices if the local area devices fail to activate after an appropriate time delay, is not only valuable but essential and should be incorporated into the system.
8. "Feed Forward" allows the local critical devices to remain enabled, even though the local interlocks have tripped, if the upstream critical devices are off. The committee feels the use of "Feed Forward" will

complicate the system logic and testing with little benefit to operations. The committee recommends this feature not be implemented.

9. The committee feels that, where an area is common to two systems, the gates, critical devices, etc. be monitored by separate switches for each system and independently controlled (enabled) by both systems. This preserves the isolation of the systems and ensures modularity and independence during maintenance and testing.

10. The system design should incorporate "safety system test" modes to allow the efficient testing of interlock components while ensuring the critical devices are not enabled or without adjacent systems being affected.

Along this line, the committee feels the use of a "system-shut down key" is needed, however, the system should never ignore the basic safety of the system. If the "system shut-down key" is actuated, the system should still monitor the gates or attempt to remove the permits to the system. The committee feels that by ignoring the gates the system would have a built in failure mode that would cause the loss of protection. The key could, for example, only release the door solenoids. It is recognized that this failure would only effect one loop. For reasons previously explained, operation with one loop bypassed must be avoided.

11. The committee recommends additional diversity be employed in the control of the critical device power supplies. It would be possible for one loop to remove the firing pulses to the power supply while the other opens the contactor. It is understood by the committee that the "Reachback" system would ensure the device functioned as commanded. This could be ensured by watching the voltage & current output of the power supply.

12. It is a concern to the committee that the AGS and RHIC complexes use different warning alarms for the same function (Beam Enabled). It

has long been a desire (and possibly a DOE directive) to have a common warning tone for a hazard at a given facility. It is thought that operator/personnel confusion would be avoided if the warning sound for the beam enabled warning was the same at both the AGS and RHIC complex. The committee was confused initially by the use of the term "*Radiation*" for the "Beam Enabled" warning strobe and alarm. The committee recommends renaming the alarm and strobes to eliminate potential confusion between beam enabled and a radiation trip.

13. The committee recommends that the programming personnel for the PSS review and adopt, as appropriate, the techniques contained in;

SP-84(ISA) Programmable Electronic Systems for Safety Applications and

Programmable Electronic Systems for Use in Safety Applications, UK. Health and Safety Executive.

This recommendation occurs due to questions concerning the programming method employed in which a common subroutine is used to process several different types of signals. The committee believes this is not good practice, as defined in the above documents, since a change in the subroutine could have undetected effects on other unrelated parts of the program.

14. The committee questions the need for dual UPS systems. It was felt by the committee that the UPS system is not safety critical but rather an operational issue since it prevents down time due to power grid losses. During these periods other systems would likely cause the beam to be lost. The committee feels these funds could be better applied in other areas of the system.
15. The committee, while commending the concept as innovative, question the use of analog levels to represent gate status. It is believed by the committee that this method of detection, when coupled with the

electrical noise generated by SCR power supplies and experimental equipment, may result in poorer system availability than a more conventional approach. The committee strongly believes the cost of extra cabling to the local RIO unit would be far offset by the lost time due to inadvertent trips of the gate system. The same argument is made for the crash switches. The committee recommends that a conventional approach to the monitoring of gates and crash switches be employed.

16. The concept of an adaptive voltage monitoring system was proposed. This would allow the safety system to change the trip points of the gate monitor portion of the PSS as the voltage driving the gates changed. The committee believes that this would unnecessarily complicate the testing and verification of the system. The committee *rejects* this proposal.
17. Interlock testing requirements are set forth in section V. paragraph D. of the BNL ES&H Standard 1.5.3 "Interlock Safety for Protection of Personnel". The PLC based design of the proposed RHIC Personnel Protection Safety System departs from the past practice at the AGS and elsewhere at BNL. The review committee recommends that particular attention be paid to the following matters since the critical factors involved will be different with PLC based systems compared to those using relay logic.
 - a. Modular design is particularly important in large systems so that maintenance and testing can be done in units of manageable size. Transmission of data and critical device permits between modules will determine whether changes in an area under repair or test can compromise the performance of other modules.
 - b. The extent of testing required after repair or replacement of parts of the system should be decided as a matter of policy so that this is not left to personnel doing the repair.

- c. The circuits monitoring gates, crash devices, and ODH sensors use multiple level analog signals. Tests of these circuits should verify that signal margins are adequate to reliably register all trip conditions.

Discussion

In recommendation number one the committee felt that since the radiation safety system was needed during running periods, and the ODH system was needed during access periods, the time for maintenance and testing of the systems did not exist. The entire ring would have to be down and the magnets emptied in order to ensure an ODH problem did not exist. Furthermore, the testing would become unduly complex to ensure problems in coding or system performance did not affect both systems. If the two systems were separated the radiation safety system could be tested during down periods without affecting the ODH safety.

In item number two, the committee wanted to ensure that proper attention was afforded the situation where the ODH system could have a detrimental effect on the fire protection by providing oxygen to a smoldering fire. It is also important to choose the type and placement of fire protection and ODH sensors.

In item number three, the committee (while on our tunnel tour) found that access to the control for the ventilation fans was not restricted and the fan controls were not protected from undetected shut-down for maintenance. It was further noted that since this item may have repair done by another group (such as a facility maintenance group) the operation, control, and maintenance of these devices be tightly controlled. This is especially true due to the need for these fans to be fully functional when an ODH condition is detected. It was further determined that these devices must somehow be checked for proper functioning when commanded to operate and at regular intervals.

In item number four the committee discussed the issue of probability when discussing failures. While numbers could be determined and would show one failure in 10^n years, this only tells you

the duration between failures and not when the failure will occur. It really says that in 10ⁿ years I will only experience one failure, it does not tell you that failure can happen today, tomorrow, or 10ⁿ years from now. Given this uncertainty in failure and given that switch failures cannot be detected unless the gate is opened, the committee feels the concept of running with one loop failed is not consistent with the rules required by DOE or any standards organization for personnel safety.

In item number five the committee felt this was mandatory as part of "good engineering practices". It is better to design in the features at the beginning than to fudge them in later.

In item number six the committee is stressing the obvious but necessary items to cover with policy decisions.

In item number seven the committee considers this good system design practice as something relatively easy to do which adds to system safety.

In item number eight the committee decided the complication far outweighed the benefits. One could hypothesize a situation where the upstream most device is off and all others therefore are left on. If the upstream device then goes on, but the others should be off, the system must go through several gyrations to settle down on which device should be off to allow the others to be on. This complicates testing since all of those conditions would have to be certified as working properly during system tests.

In item number nine the committee was again quoting good design practices. Two systems should remain as independent as possible to ensure no multiple system failures could be caused by a single device. Agreement with this point was expressed by the Brookhaven staff at the close-out meeting.

In item number ten the committee expressed the opinion that providing test modes that ignore the safety of the system could be dangerous for a number of reasons. One item that must be kept in mind is the possibility that the PLC "somehow" gets into test mode during normal running. Again one could offer a failure in which the PLC finds itself in some part of the test code and therefore ignores all safety inputs and is quite happy to do so.

In item number eleven the committee was again attempting to stress the separation of the two "loops" or redundant paths. In one of the slides the committee was shown a drawing called "IOBLOCK" "Critical Device Communications" in which the two PLC systems are depicted interacting with one device in the Critical Device Power Supply. The committee is advocating an approach in which two different means of controlling the device are used and the shutdown functions controlled by the 1791-BBC's are completely separated.

In item number twelve the committee is expressing a concern for the non-standardization of alarms. This is in the interest of minimizing the number of confusing alarm tones that an operator or experimenter has to remember. As a general comment, Brookhaven may wish to review the warning tones used at all facilities for standardization.

In item number thirteen the committee is expressing its desire for the adoption of the programming techniques spelled out in two related documents. It should be noted that this item was strongly recommended by the committee members who have operational experience with PLC based systems. The intent is to enforce proper technique to avoid programming errors that could be detrimental to the safety of the system.

In item number fourteen the committee saw this as an unnecessary redundancy that adds to the maintenance load and does not provide any significant safety. The use of one system, properly installed, does not

have a negative effect on the PLC safety system. If it is argued that this is needed to provide safety coverage for the ODH system during a power outage, then it may be valid but a more thorough look at the system would be needed.

In item number fifteen the committee's main quandary was not safety related but rather operational with a secondary safety consequence. In opening a gate as shown in the chart "MYEXPLE.XLS" it appears the change in gate closed to gate open voltage is at most 1.99 volts and can be as small as 0.52 volts. In the collective experience of the committee it was felt that the voltage difference may be too small. This could cause "false" trips of the system due to noise pickup from power supply pulses in the magnet system. If this caused a loss of the permits a significant radiation loss could occur. It should be noted that the relationship of what is called gate 1, 2, or 3 was not easily determined nor was a more detailed understanding obtained. This item is expressed as a possible operational problem which should be examined more closely.

In item number sixteen the committee's main concern is that of testing and ensuring the proper operation of the system. If the voltages for the sensing are "adaptive" in that the system can change the levels that are considered good, the system is far more difficult to test and may offer compromised safety if a mistake is made.

In item number seventeen the committee is again expressing general design criteria that must be adhered to for a successful and safe PLC safety system.

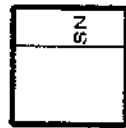
Attachments

IOBLOCK drawing

MYEXPLE.XLS

Acceptance signatures of committee members.

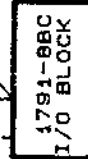
SLC500



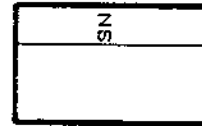
UP TO 8
PER SN



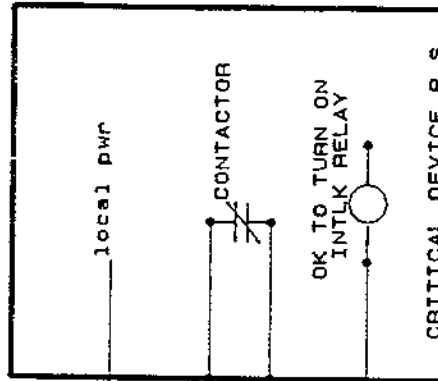
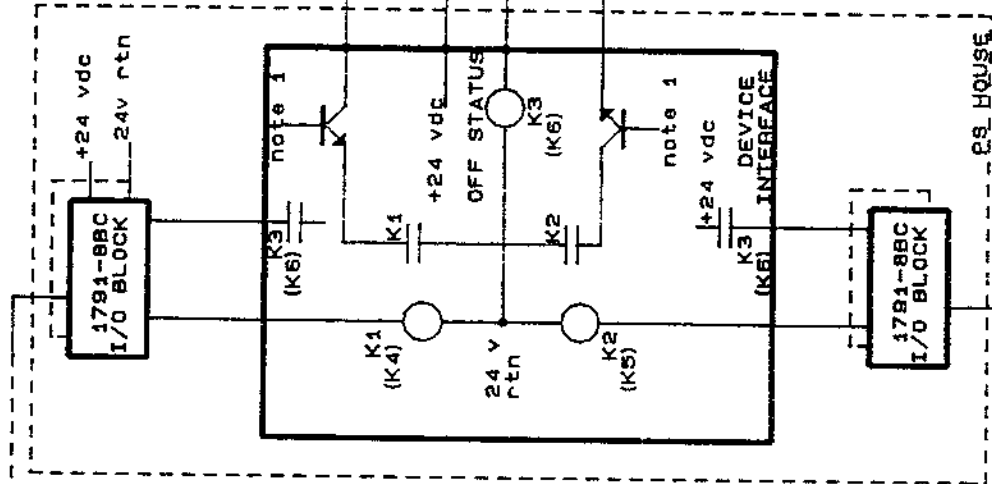
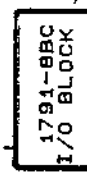
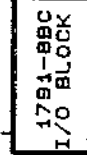
8 INPUTS
8 OUTPUTS



PLC-5



shielded
twisted pair



NOTES

1. To be driven by a "heartbeat" detection circuit whereby loss of an output bit from 1791 opens switch.

CRITICAL DEVICE COMMUNICATIONS

Size Document Number
A IOBLOCK

REV

am

Date: February 23, 1995 Sheet of

MYEXPLE.XLS

[illegible]

I have read the final committee report on the RHIC Personnel Safety System at Brookhaven National Laboratory and agree with the report as presented.


Name Howard Casebolt

Affiliation Fermilab - Accelerator Div.

Signed *HC Casebolt*

Date 5/23/95

I have read the final committee report on the RHIC Personnel Safety System at Brookhaven National Laboratory and agree with the report as presented.

Name THOMAS S. DICKINSON
Affiliation BNL - NSLS
Signed 
Date 5/31/95

MAY-25-'95 THU 10:07 ID:
MAY-23-1995 13:51 FROM FERMILAB EE/RFD

TEL NO:
TO

#048 P02
92526123 P.02

I have read the final committee report on the RHIC Personnel Safety System at Brookhaven National Laboratory and agree with the report as presented.

Name John R Forrestal

Affiliation Argonne National Lab. Advanced Photon Source

Signed *JR Forrestal*

Date 5/24/95

C.E.B.A.F.

TEL No.804-249-7352

May 30,95 13:41 No.008 P.01

MAY-25-1995 09:58 FROM FERMILAB EE/RFD

TO

918042497352 P.02

I have read the final committee report on the RHIC Personnel Safety System at Brookhaven National Laboratory and agree with the report as presented.

Name HENRY ROBERTSON

Affiliation CEBAF

Signed 

Date 5-20-95

BROOKHAVEN NATIONAL LABORATORY

RHIC Project

MEMORANDUM

DATE: October 12, 1995

TO: R. Frankel

FROM: S. Ozaki *S. Ozaki*

SUBJECT: Implementation of recommendations from the External Review of the RHIC Safety System

I agree with your position on the External Review Committee recommendations and the assessment of the Radiation Safety Committee in the memoranda from R. Frankel to A. Etkin dated July 21, 1995 and A. Etkin to S. Musolino, dated October 11, 1995. Since you conclude that the items which will not be adopted in design and operation of the system relate only to reliability and not personnel safety, it is up to your discretion to follow items 1, 14 and 15.

cc: A. Etkin
M. Harrison
H. Kahnhauser
S. Musolino
K. Reece
RSC File (M. Heimerle)

BROOKHAVEN NATIONAL LABORATORY
RHIC PROJECT
RADIATION SAFETY COMMITTEE
RHIC SUB - COMMITTEE

To: S. V. Musolino

From: A. Etkin 


Date: October 11, 1995

Subject: Response to External Review of the RHIC PASS

At a meeting of the Sub-committee on September 18, 1995 the response to the report of the External Review Committee for the RHIC PASS by R. Frankel was discussed. It was concluded that the items that were not accepted in total do not represent radiation safety issues for the ATR tests and that the operational issues will be studied during the upcoming ATR tests.

xc:, R. Frankel, M. A. Harrison, S. Ozaki, R. K. Reece

RHIC Project Safety Section

to A. Etkin
from R. Frankel 
date 21 July 1995

Subject Recommended actions to the Committee Report On the
RHIC Personnel Safety System at Brookhaven National Laboratory
(March 7, 8 and 9, 1995)

I recommend that RHIC adopt Committee recommends numbers
2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16 and 17. These recommendations
are to be in place prior to the 1996 Sextant Test.

I further recommend the following initial response to items 1 and
15 and the proposed alternative to item 14.

Item 1 "Separate the ODH and Radiation Safety Systems"

" the committee recognizes the importance of the ODH system and feels the
two systems serve critical but separate functions."

There are four issues here: software complexity and performance, verification
and testing complexity, implementation costs, equipment availability.

In my opinion the most telling argument in favor of this committee
recommendation goes as follows: you most need your Radiation Safety System
when you have Beam-enabled and at that time, because personnel are excluded
from the magnet enclosure, you have less need for the ODH system. Conversely,
when you are in Restricted Access and have personnel in the magnet enclosures
you are at maximum sensitivity to ODH Hazards, but you are exposing people to
minimum Radiation related risks. This thesis is indeed generally correct, but as
with most real world problems, the devil is in the details. At all times, RHIC is
still required to protect its personnel and *visitors* (invited or not) from accidental
exposure to residual as well as prompt radiation, as well as a need to protect
personnel and visitors who work in or enter our Cryogenic and Service buildings
from ODH hazard. Under any but the most rare circumstance, this means **both** a
functioning Access Control system and a functioning ODH Safety System.

The expected size of our ODH code will be some 500 words and perhaps 40 ladder rungs. Translating this into more generally understandable terms; it will consume only five percent of processor capacity. This number is as low as it is because of the bus-like nature of our Supervised field wiring system. An analogy can be drawn between the relative efficiency of implementing accelerator timing with a "time-line" as opposed to using a random collection of timing generators and interconnects. The software complexity issue, from a technical standpoint, is not significant.

The verification argument is best addressed by accepting that the combination of the two protection systems will indeed make verification of changes more difficult and time consuming. However, it can also be expected that after an initial "turn-on" period that there will be fewer and fewer changes which need to be validated. This point of view is also supported by our use of built-in test and maintenance modes, which are being implemented to minimize the need for software rewrites.

Since this committee recommendation is offered in the context of cost and operational efficiency rather than as mitigating a potential safety hazard, I would like to offer the following cost analysis. Item 4 of the Recommendations and Comments section "categorically rejects" continued operation of the RHIC complex "with only one Personnel Safety loop active ...". Therefore I will assume that any ODH system must be redundant. This means that twelve additional PLC processors with their associated power supplies, RIO modules and Racks need be added to the current design. The likely impact to the project is ~ \$100,000 in direct costs as well as added additional design, installation and housing costs.

If an additional \$100,000 would result in reduced down time at RHIC, I would consider it money well spent and advocate its expenditure, but in separating the systems we will also almost double the amount of equipment which must function correctly for continued operation. Irrespective of one's opinions as to expected equipment availability; adding twice as much hardware is likely to halve the mean-time-to-safe-failure of the system.

Item 14, "review the need for dual Uninterruptable Power Supplies"

The committee states that the use of these units is not safety-critical but rather operational. It further states that these funds could better be spent elsewhere.

The project has benefited from recent advances in UPS technology and subsequent cost reductions which have come about as a result of wide-spread deployment of LAN servers.

These units are available up to roughly 1.5 KVA at low cost. If we were to replace the individual UPS units used at a division site with a common unit large enough to supply both divisions we would not be able to purchase a UPS intended for Server service and would actually pay more money for a single larger unit of the same capacity as compared to two smaller units sized to the capacity of a Division PLC.

Item, 15 "Adopt more traditional Gate and CRASH switch sensing"

"The committee, while commending the concept as innovative, question the use of analog levels to represent gate status. It is believed by the committee that this method of detection, when coupled with the electrical noise generated by SCR power supplies and experimental equipment, may result in poorer system availability than a more conventional approach. The committee strongly believes the cost of extra cabling to local the local RIO unit would be far offset by the lost time due to inadvertent trips of the gate system. The same argument is made for the crash switches. The committee recommends that a conventional approach to the monitoring of gates and crash switches be employed."

The committee expresses concern that the proposed system of using multiple analog levels as a measure of Gate status "may result in poorer system availability than a more conventional approach" (because of greater susceptibility to electrical noise).

The BNL Fire-Protection Engineer informs me that systems similar to what we have proposed are currently in use for industrial fire protection, and have been for "decades". These fire systems monitor for open circuits, short circuits and ground connection while indicating which station is alarming. Normal practice is to limit the number of "stations" from one to more than thirty based on critically-of-function. Our proposal for Gate and CRASH monitoring, limits a circuit to three Gates or five CRASH switches per wiring loop. Furthermore the CRASH circuits will only be used to indicate whether we have one or more than one activation.

I strongly believe that our design has more than adequate noise margins to reliably measure Gate and CRASH status.

Since the committee did not question the safety of this system, but its availability, I recommend that we continue with the current design through the ATR test period and gather data as to whether we have sufficient noise margins in an actual field test. If we see reliability problems the design can be subsequently changed so as to follow the committee recommendation. If performance is good during the ATR test we can continue our evaluation during the Sextant Test period. The final design for the Collider enclosure itself can be made at that time.

I suggest this course of action for the following three reasons:

- 1) I question the committee assertion that "the cost of the extra cabling to the local RIO units would be far offset by the lost time due to inadvertent trips of the gate system." My admittedly fast calculations (50,000 feet of additional cable) suggest a cost of \$150,000 to \$250,000 when the extended cost of more and different modules, crates, cabinets, cables, conduit, ducts and four times the programmed cost of installation, interconnect and test time are included. Additional costs will accrue because of engineering and software redesign.
- 2) The proposed system also provides extensive feedback about the state of the Gate and its associated wiring. It can for example tell if the cable is open circuited or grounded, short circuited. This approach is *safer* than point to point wiring, which can only tell if the circuit in question is open. Another important advantage is that fewer wires and modules need be tested to verify the system functionality, after preventative or corrective maintenance.
- 3) The last issue is schedule, at this point in the Project, ATR readiness would be placed in doubt. Redesigning the hardware and software and obtaining new and different components prior to our and G-2's scheduled run is very chancy.

To spent a lot of money *and* to jeopardize the schedule to compensate for the possibility that another approach *may* give better availability in the long run is a bad gamble. The notion of field testing and evaluation of performance before committing to the Collider enclosure wiring is our best option at this point.